

AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph from page 20 line 6 to page 21 line 19 with the following amended paragraph:

A1
The part of the executing apparatus 200 that relates to the usage (e.g., reproduction) of digital contents includes the following functional components. A random number storing unit 201 stores a random number in a manner that prevents its stored content being read or changed from outside the executing apparatus 200. This random number storing unit 201 can be composed of a circuit that does not have an interface allowing access from outside the executing apparatus 200. A first decrypting unit 202 decrypts an encrypted supplementary key stored on the recording medium 100 using the random number stored in the random number storing unit 201 to obtain a supplementary key. A second decrypting unit 203 decrypts the encrypted usage conditions on the recording medium 100 using the supplementary key obtained by the first decrypting unit 202 to obtain the usage conditions. A unique key storing unit 209 stores the unique key SK, considered a type 3 key for encryption and decryption, in a manner which prevents the unique key from being read or written from outside the executing apparatus 200. A third decrypting unit 204 decrypts an encrypted digital content using the unique key stored in the unique key storing unit 209 to obtain a digital content. A digital content using unit 205 uses the digital content ("using" meaning "reproducing" in the case of audio or image information) decrypted by the third decrypting unit 204. A usage condition examining unit 206 examines the usage conditions decrypted by the second decrypting unit 203 when a digital content is to be used, judges whether the usage of the digital content is permitted, and informs the third decrypting unit 204 whether or not decrypting is permitted for the digital content. A usage condition updating unit 207 updates the usage conditions, such as the remaining number of

A1 permitted executions, in accordance with the usage of digital contents. A supplementary key generating unit 210 generates a new supplementary key in accordance with the usage of digital contents. A first encrypting unit 208 uses the supplementary key generated by the supplementary key generating unit 210 to encrypt the usage conditions, which have been updated by the usage condition updating unit 207, and so updates the encrypted usage conditions on the recording medium 100.
